HACKERUSA

Knowledge, Experience, Responsibility

Cyber Security Risk Management & Assessment

40 Hours

Sorting Stage

360 Hours

Extended Course

Cyber Security Risk Management & Assessment

Since our establishment over 20 years ago, we have been Israel's flagship IT-and-cyber-security academy (a 'Microsoft Silver Partner' and an EC-Council accredited institution), with over 4,000 graduates per year. Thanks to our world-class program and highly networked career-placement services, 85% of our graduates in Israel land strategic positions in the high-tech market, and we are incredibly proud of the thousands of industry experts whose careers started here. They are a testament to our commitment to our students' futures.

In recent years, demand for cyber security professionals has surged. Companies are looking to integrate cyber-risk management into day-to-day operations and maintain a prepared response to any cyber security incident to ensure that all assets and data are protected.

The Cyber Security Risk Management & Assessment program is suited for IT Managers, CIO, CISO, Advanced IT Consultants, and Risk Evaluation Employees.

Objectives

Students who complete this program will be able to perform quantitative and qualitative risk assessments. Our mission is to transform our students into first-class cyber-security risk managers within one of three main channels: analysis, assessment, and mitigation. Identifying threats as well all soft spots and providing protection are the core skill sets that this program builds through intensive hands-on training that familiarizes students with case studies, frameworks, and live risk-management simulations.

Prerequisites

- Windows Servers
- Active Directory
- TCP / IP
- Switches
- IT Basics
- Risk Evaluation Experience
- Professional evaluation admissions exam

Benefits

- Mastery of risk evaluation through real life case studies
- Industry-oriented curriculum designed and delivered by industry experts
- Focus on team-management and risk-evaluation processes
- 85% industry job placement success rate in Israel through HackerU's career services within 60 days of graduation
- Trial period with minimal financial risk

Course Methods

Instructional Methods

Class lectures and labs

Evaluation and Skills Assessment

The instructor will evaluate all of the students according to their attendance; performance on labs, quizzes, and exams; class participation; and completion of homework assignments.

Course Outline

- **Pre-training Course:** The 40-hour pre-training course builds the fundamentals that are necessary to acquire the higher-level knowledge and skill sets taught in the course. At the end of this course, students will undergo two evaluations: a written exam and an evaluation by the instructor. After the evaluation, the student and instructor will decide together whether the student should proceed to the extended course. Students who do not proceed will be refunded 75% of the Pre-Training Course tuition

  Tuition: $1,000

- **Extended Course:** 360 hours of lectures and labs.

  Tuition: $17,000

Course Grade

30%	Final exam
20%	Midterm exam
20%	Presentations / Labs
20%	Homework assignments
5%	Quizzes
5%	Class participation / Attendance

Certifications

- HackerU Certified Risk Manager

Curriculum

01 Cyber Security
40 Hours

- Data breaches
- Personnel Security
- Business Continuity and Disaster recovery
- Case Studies of Policy, Usage of Norms and Standards, Procedure and Processes
- Security governance
- Protection control types
- Security Frameworks, Models, Standards, and Best Practices
- Computer laws and crimes
- Intellectual property

02 Cloud Security
40 Hours

- Introduction to Cloud Computing
- Challenge of the Cloud Security
- Vendors and Comparison
- Infrastructure Concepts
- Key point of the Security
- Compliance and Legal Consideration
- Disaster Recovery Operations
- Risk, Audit and Assessment
- Intrusion Detection and Incident Response

03 Cyber Risk Management
100 Hours

- Cyber Risk management: ISO27005, COBIT
- Audience of Cyber Risk
- Risk Governance
- Risk Evaluation
- Risk Response
- Cyber Risk Tools
- KRI (Key Risk Indicators) and Reporting Activities
- Threat Modeling
- Case Study

04 Asset Security
20 Hours

- Information Life Cycle
- Information Classification and Protection
- Information Ownership
- Protection of Privacy
- Information Retention
- Data Security Controls
- Data Handling Requirements

05 Security Engineering
40 Hours

- System architecture
- Trusted Computing Base and Security Mechanisms
- Information Security Software Models
- Assurance Evaluation Criteria and Ratings
- Certification and Accreditation Processes
- Distributed Systems Security
- Cryptography Components and their Relationships
- Steganography
- Public Key Infrastructure (PKI)
- Site and Facility Design Considerations
- Physical Security Risks, Threats, and Countermeasures
- Electric Power Issues and Countermeasures
- Fire Prevention, Detection, and Suppression

06 Communication and Network Security
20 Hours

- OSI and TCP/IP Models
- Protocol Types and Security Issues
- LAN, WAN, MAN, Intranet, and Extranet Technologies
- Cable Types and Data Transmission Types
- Network Devices and Services
- Communications Security Management
- Telecommunications Devices and Technologies
- Remote Connectivity Technologies
- Wireless Technologies
- Network Encryption
- Threats and Attacks
- Software-defined Routing
- Content Distribution Networks
- Multilayer Protocols
- Convergent Network Technologies

07 Identity and Access Management
20 Hours

- Identification Methods and Technologies
- Authentication Methods, Models, and Technologies
- Discretionary, Mandatory, and Nondiscretionary Models
- Accountability, Monitoring, and Auditing practices
- Registration and Proof of Identity
- Identity as Service
- Threats to Access Control Practices and Technologies

08 Security Assessment and Testing
40 Hours

- Internal and Third-party Audits
- Vulnerability Testing
- Penetration Testing
- Log Reviews
- Synthetic Transactions
- Code Reviews
- Misuse Case Testing
- Interface Testing
- Account Management
- Backup Data Verification
- Disaster Recovery and Business Continuity Testing
- Security Training and Awareness
- Key Performance and Risk Indicators
- Reporting
- Management Review
- Case Study and Technical Overview

09 Security Operations

40 Hours

- ITIL Overview
- Operations Department Responsibilities
- Administrative Management Responsibilities
- Assurance Levels
- Configuration Management
- Physical Security
- Secure Resource Provisioning
- Network and Resource Availability
- Preventative Measures
- Patch Management
- Incident Management
- Recovery Strategies
- Disaster Recovery
- Business Continuity Planning and Exercises
- Liability
- Investigations
- Personal Safety Concerns
- Case studies of Organizations, Procedures, and Processes

10 Software Development Security

40 Hours

- Common Software Development Issues
- Software Development Life Cycles
- Vendor and Comparison
- Secure Software Development Approaches
- Development/Operations Integration (DevOps)
- Change Control and Configuration Management
- Security of Code Repositories
- Programming Language Types
- Database Concepts and Security Issues
- Malware Types and Attacks

Course Summary

Module	Hours
Cyber Security	40
Cloud Security	40
Cyber Risk Management	100
Asset Security	20
Security Engineering	40
Communication and Network Security	20
Identity and Access Management	20
Security Assessment and Testing	40
Security Operations	40
Software Development Security	40
Total	**400**

HACKERUSA

Knowledge, Experience, Responsibility